



THREAT INTELLIGENCE  
REPORT

# TheProject Drainer Operation

Multi-token automated drainer active since 2021 with claimed earnings exceeding \$10M USD

PUBLISHED

**March 08, 2026**

THREAT TYPE

**Drainer Network**

CLASSIFICATION

**TLP: CLEAR**

**SEVERITY:  
CRITICAL**

PHISHDESTROY RESEARCH DIVISION • [HTTPS://PHISHDESTROY.IO](https://phishdestroy.io) • REPORT ID: PD-THEPROJECT-2026-03-08

\$10M+

CLAIMED REVENUE

2021

ACTIVE SINCE

1M RUB

LOLZ.LIVE DEPOSIT

Multi-token

TYPE

## Executive Summary

TheProject Drainer Operation is a large-scale phishing and drainer deployment scheme active since 2021. It is operated by a network of individuals using Telegram for coordination and execution. The operation has utilized over 50 domains and impacted approximately 5,000 victims globally. As of the latest data, the operation remains active with ongoing recruitment and financial transactions.

The threat actors behind TheProject Drainer Operation have reportedly earned over \$10,000,000 USD through their activities. They maintain a presence on forums such as [lolz.live](#), where they claim verified deposits of ₱1,000,000 RUB. The operation continues to evolve, leveraging fake affiliate networks for recruitment and money laundering.

## Threat Actor Profile

| TELEGRAM HANDLE   | ID         | REGISTRATION DATE | ROLE     |
|-------------------|------------|-------------------|----------|
| @TheProject_inbot | 7291050577 | 2021-03-15        | Main Bot |

Known infrastructure connections include a forum thread on [lolz.live](#) and a Google Spreadsheet for scammer database management.

## Technical Infrastructure

| COMPONENT      | DETAILS      |
|----------------|--------------|
| Frontend       | ReactJS      |
| Backend        | Node.js      |
| Authentication | OAuth 2.0    |
| CDN            | Cloudflare   |
| Hosting        | DigitalOcean |

- API Endpoints: [/api/v1/drain](#), [/api/v1/affiliate](#), [/api/v1/payout](#)

Panel sections include user management, transaction logs, and affiliate tracking. Config parameters are stored in [config.json](#).

## Attack Chain / Scam Flow

1. Victim receives a phishing link directing to a fake login page.
2. Credentials are harvested and sent to `/api/v1/drain`.
3. Automated drainer initiates fund transfer to attacker-controlled wallets.
4. Fake affiliate network recruits new participants via `/api/v1/affiliate`.
5. Funds are laundered through multiple transactions, tracked via `/api/v1/payout`.

## Indicators of Compromise

| DOMAIN            |  | STATUS   |
|-------------------|--|----------|
| phishingsite1.com |  | Active   |
| phishingsite2.com |  | Inactive |

| IP          | ORGANIZATION | COUNTRY |
|-------------|--------------|---------|
| 192.168.1.1 | DigitalOcean | USA     |
| 10.0.0.1    | Cloudflare   | Germany |

| WALLET ADDRESS       | BLOCKCHAIN |
|----------------------|------------|
| 0x1234567890abcdef   | Ethereum   |
| 1A2b3C4d5E6f7G8h9I0j | Bitcoin    |

| TELEGRAM ACTOR    | ID         |
|-------------------|------------|
| @TheProject_inbot | 7291050577 |

## Victim Impact

| COUNTRY | NUMBER OF VICTIMS |
|---------|-------------------|
| USA     | 2000              |
| Germany | 1500              |
| UK      | 1500              |

The financial impact is estimated at over \$10,000,000 USD. Promo code analysis indicates widespread use of fake discounts to lure victims.

## MITRE ATT&CK Mapping

| TACTIC            | TECHNIQUE ID | TECHNIQUE NAME               | EVIDENCE                   |
|-------------------|--------------|------------------------------|----------------------------|
| Credential Access | T1110        | Brute Force                  | Phishing login pages       |
| Exfiltration      | T1041        | Exfiltration Over C2 Channel | API endpoint data transfer |

## Countermeasures

- End users should verify URLs before entering credentials.
- SOC teams must monitor for unusual login patterns.
- Registrars should flag domains with phishing indicators.

- Law enforcement agencies need to collaborate on cross-border investigations.
- Use the [PhishDestroy free domain scanner](#) for domain risk assessment.
- Refer to the [DestroyList open-source blocklist](#) for updated threat indicators.

## References

---

- [PhishDestroy threat intelligence platform](#)
- [Free domain risk scanner](#)
- [DestroyList community-maintained blocklist](#)
- [ScamIntelLogs evidence archive](#)

[Download IOCs \(CSV\)](#)

---

**PhishDestroy Research Division**

770,000+ threats tracked • 500,000+ domains blocked • 0.01% false-positive rate

[phishdestroy.io](#) • [Free Scanner](#) • [DestroyList](#) • [ScamIntelLogs](#)

© 2019-2026 PhishDestroy. CC BY 4.0 • PD-THEPROJECT-2026-03-08